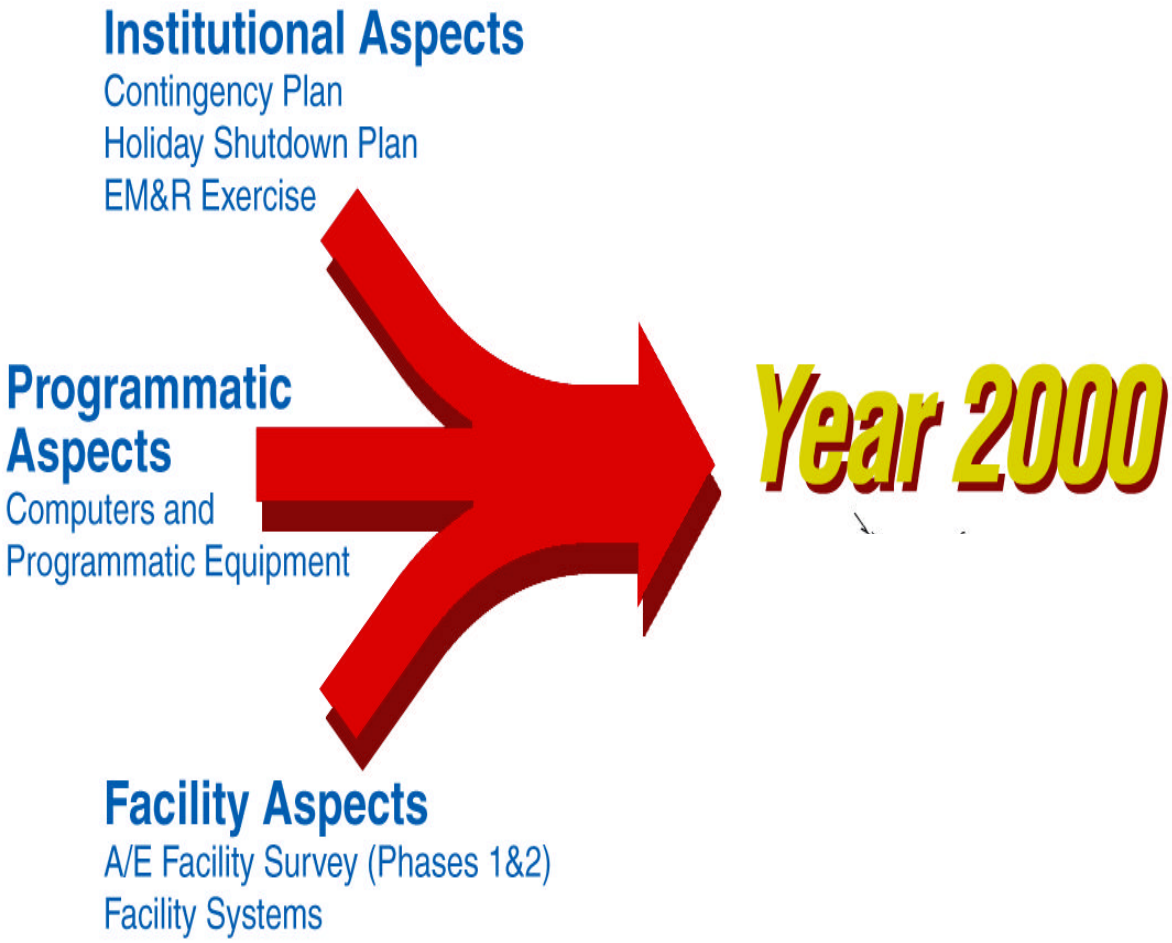
Year 2000 Project Plan



Version 2.0 DRAFT December 1999: Appendix G contains updates on progress made implementing original Project Plan.

Information Architecture
Year 2000 Project
Los Alamos National Laboratory

Table of Contents

List of Tables

Appendices

CHANGE CONTROL PAGE

Version number	Date issued	Reviewed by	Changes
2.0	December 1999	D. Weir and editor	Added this change control page Fixed minor errors The original Year 2000 Project Plan was written in December 1998. An update is included in this version as Appendix G. The project plan schedule has not been included in this version. Revisions have been made in text as well to bring readers up to date on what has happened.

Year 2000 Project Plan

1.0 Scope

Preparing for Year 2000 is the responsibility of everyone at Los Alamos National Laboratory. In this document, the Year 2000 Project office outlines a comprehensive approach to what we will do to ensure a smooth, and safe, transition to the Year 2000.

The Year 2000 Project at the Laboratory is a three-pronged effort covering the institutional, facility, and programmatic aspects of the Year 2000 issue. The Facilities Planning team ensures the readiness of buildings and infrastructure systems, contingency plans for the Laboratory as a whole, and coordinates with the Los Alamos community and external service and utility providers. The Year 2000 Council deals primarily with programmatic computer issues, and its members serve as communication coordinators. Overseeing all these efforts are the Year 2000 senior management sponsors, Charlie Slocomb, CIC Division Director, and Dick Burick, Deputy Laboratory Director for Laboratory Operations. The effort is supported by the Year 2000 Project Office staff. Section 3 of this report outlines all tasks and responsibilities for Year 2000.

The FY99 cost for Year 2000 preparations at the Laboratory is now estimated to be about $15 million. This figure was not tracked as a separate item in the Laboratory's financial system.

1.1 Programmatic

All line managers must work with their staff to ensure that the systems that support their organization will work in the Year 2000. This includes computer systems, their applications, and the embedded systems that collect data and manage programmatic equipment.

1.2 Facilities

The facility managers (FMs) must ensure that their building systems will not be affected by Year 2000 failures. January is the coldest month of the year, and we must make plans to ensure that there is no damage to buildings or equipment, and that people in the facility will be safe.

1.3 Safety-related systems

Facility Managers responsible for nuclear and high/moderate hazard facilities must assure that the "safety-related" systems in those facilities are Year 2000 ready. A "safety-related" system is a system that is or is expected to be included in the authorization basis document for that facility.

1.4 Institutional

The institutional aspects of Year 2000 involve planning for the "millennium hour." Many systems could fail one time, at 00:00 on January 1, 2000, while the computer clock breaks as it tries to move forward. Because of the potential risks of a electrical power fluctuations or failures, we must ensure that the Laboratory's security, safety, and environment are not compromised. The Laboratory's Year 2000 Business Continuity Plan describes the plans for the use of the power plant in case of problems with the grid.

1.5 Weapons Manufacturing, Test, and Acceptance Compliance

The DOE/AL/WSD, during the Quality Assurance Survey (QAS) performed on November 4-5, 1998 identified a concern relative to the weapons Year 2000 compliance and requested the development of a comprehensive list of computer/computer controlled equipment and systems that can affect weapons manufacturing, test, and acceptance (MTA) activities.

This activity was coordinated by Deb Lucero of the Weapons Quality Office. Participants from ESA, DX, NMT, and MST worked with people in their respective divisions to develop the MTA inventory, assessment, and remediation plans, schedules and progress. The MTA equipment was specially coded in the Year 2000 database. The Year 2000 database provided specialized status reports for MTA systems while allowing the Year 2000 project to have a single source for Year 2000 status information. MTA systems were reported to Laboratory management just like all other systems.

A final report was submitted to DOE/AL/WSD in order to close this audit finding.

2.0 Principles for Year 2000 Solutions

2.1 Take a Risk-based Approach

The biggest problem we face in preparing for the Year 2000 is that computers are ubiquitous and support many of our safety, environment, and security processes. We must take a risk-based approach to the problem by focusing our efforts on the critical systems first.

2.2 Focus on Critical Systems

The first areas of concern are systems that:

- Guarantee safe containment and accountability for nuclear material or hazardous chemicals
- Keep building systems operating and within an acceptable temperature range
- Provide security
- Prevent loss or damage to property and facilities
- Guarantee only authorized access to classified information
- Prevent harm to the environment
- Keep critical operations functioning

These systems require contingency plans in the event of unforeseen failures. Testing is key for ensuring the success of critical systems. GartnerGroup best-in-class companies test 60% of the functionality (including transactions, data, interfaces, and environments) of their critical systems as a risk minimization technique. Noncritical systems are only tested up to the 20% level.

2.3 Coordinate with Your Year 2000 Council Representative

The Year 2000 Council is made up of knowledgeable computer users from most divisions and program offices. This distributed approach is the best way to ensure that the Year 2000 issues are brought to the attention of the individual divisions and program offices so that they can be resolved across this complex campus-like organization. The Council representatives do not have organizational responsibility for fixing the Year 2000 problem. They are Year 2000 information resources for their groups or divisions.

2.4 Use the Web to Find Year 2000 Product Status, News, and Planning Resources

Start with the Laboratory's Year 2000 Web site, which is the fastest access to information about actions required for your computer products, and to many useful links for vendor information, test results, contingency planning, and government program status.

http://www.lanl.gov/projects/ia/year2000/

3.0 Year 2000 Responsibilities at the Laboratory

3.1 Responsibilities of Year 2000-Specific Organizations

3.1.1 Year 2000 Senior Management Sponsors

- Charlie Slocomb, CIC Division Director
- Dick Burick, Deputy Laboratory Director for Laboratory Operations

- Provide leadership, issue-resolution authority, and general program oversight
- Serve as ambassadors for the program
- Determine funding levels that will minimize Laboratory risk
- Manage and allocate funds for Year 2000 activities
- Give Year 2000 priority, urgency, and support

3.1.2 Year 2000 Project Office

- Single point of contact at the Laboratory for Year 2000 issues
  Diane Weir, Project leader; 667-9337 (drw@lanl.gov)
  http://www.lanl.gov/projects/ia/year2000/
- Provide information to DOE, UC, and other outside parties
- Coordinate Year 2000 reviews and assessments
- Lead Year 2000 Council
- Interface with Laboratory management
- Manage the institutional contingency planning
- Interface with Legal on Year 2000 issues
- Provide the Year 2000 database and tools
- Develop *Year 2000 Project Plan* (this document)
- Develop and execute Year 2000 communication plan
- Establish legal posture
- Communicate information and learning (progress and failures)
- Provide Year 2000 status to the local communities
- Participate in community events dealing with Year 2000 issues

3.1.3 Programmatic Aspects: Year 2000 Council Representatives

- Serve as single point of contact for Year 2000 issues for a division/program
- Articulate issues and raise issues to management
- Serve as an information resource for a division and facility
- Coordinate assessment activities
- Track status, reports, and schedules using the Year 2000 database
- Communicate information and learning between an organization and the Year 2000 Council
- Communicate division and group status to management
- Participate in risk ranking for the systems
- Attend Year 2000 Council meetings
- Audit Year 2000 documentation according to the guidance

3.1.4 Year 2000 Facilities Planning Team

- Develop a Business Continuity Plan (BCP) for a total* Laboratory shutdown during the 1999-2000 holiday break, by August 31, 1999. Develop a process to keep the BCP current, as revisions will occur until the end of December 1999. (The Laboratory Business Continuity Plan is available at http://int.lanl.gov/projects/ia/year2000/contin/docs/bcp-9909.pdf

- Develop and test a contingency plan for loss of infrastructure services, due June 1999; tested by August 1999**
- Tests the power plant's capability to provide power in case of a grid failure or power fluctuations.
- Conduct two Emergency Response Exercises for Year 2000
- Manage the identification of facility systems with Year 2000 issues (A/E study)
- Manage the assessment, repair, and work-around activities
- Manage the facility contingency planning activities
- Assure that FMs are addressing the problems in their facilities
- Petition for resources (money and people) to help remediate critical systems
- Escalate issues to the Facility Management Council (FMC) as necessary
- Keep Year 2000 project office informed of progress and issues

*A total shutdown is not possible. Systems that support facilities (e.g., HVAC) and Security are probably valid exceptions. All exceptions must be clearly articulated.

3.1.5 Safety-related system owners

- Manage the identification of safety-related systems based on authorization documents
- Where authorization documents do not exist, work with Sonalysts consultants to determine which systems would be defined as "safety-related"
- Identify safety-related systems with digital components that could be vulnerable to Year 2000 issues
- Assess the safety-related systems for Year 2000 impacts
- Manage the remediation activities
- Manage the end-to-end testing and contingency planning to comply with DOE guidance
- Participate in the IV&V of the safety systems
- Keep the Year 2000 project office informed of progress and issues
- Work with your division Year 2000 council representative to update the Year 2000 database with safety-related system status

3.1.6 CIC SWAT Team

The sheer volume of computers at the Laboratory requires that we develop support teams that will help solve Year 2000 problems for customers from now through 2000. The noncritical systems and individual workstations may not function properly. CIC should prepare for an onslaught of calls from customers with Year 2000 problems. A SWAT (special weapons and tactics) Team from CIC-2 (desktop), CIC-6 (consultants), CIC-13 (Lab-wide systems), and CIC-15 (database technologies) should be chartered in early 1999 to learn about the problems customers will have and devise strategies and solutions that help customers solve their problems quickly. The better CIC is prepared, the faster customers can be productive. CIC SWAT team was chartered and submitted a project plan (see Appendix H)

3.2 Responsibilities of All Laboratory and Support Organizations

3.2.1 Divisions and Programs

- Assure Year 2000 readiness for your organization
- Allocate resources (money, people)
- Ensure contingency plans exist for critical systems in your groups
- Appoint and empower Year 2000 Council representatives
- Monitor Year 2000 progress for your organization

3.2.2 Groups

- Perform the inventory and assessment for Year 2000 readiness

- Evaluate risk for system failure and interruption
- Prioritize systems
- Do planning: determining resource needs, scheduling, and executing Year 2000 renovation, testing, and implementation
- Allocate resources (money, people) for evaluations and repairs
- Develop contingency plans for your operations
- Prepare Year 2000 documentation according to the guidance (see Appendix A)
- Communicate with Year 2000 Council representative on Year 2000 problems, issues, and progress

3.2.3 Facility Managers

- Participate in the facility evaluations by the contracted Architect/Engineering (A/E) Year firm
- Evaluate facility system risk
- Prioritize facilities and facility systems
- Do planning: determining resource needs, scheduling and executing Year 2000 renovation, testing, and implementation
- Allocate resources (money and people) for evaluation and repairs
- Develop contingency plans for each facility
- Prepare Year 2000 documentation according to the guidance (see Appendix A)
- Communicate with Year 2000 Council representative on Year 2000 problems, issues, and progress
- Keep divisions and groups in the facility informed

3.2.4 System Administrators and Applications Developers

- Assist with developing system inventory
- Assess systems and applications for Year 2000 problems
- Remediate, test, and implement the systems, networks, and applications that need Year 2000 repairs
- Serve as a resource for the users' Year 2000 repairs, questions, and issues
- Keep Year 2000 Council representative informed (Year 2000 problems, issues, and progress)
- Escalate issues to group management

3.2.5 Employees and Contractors

- Assume responsibility for equipment and systems required to perform assigned job
- Assure that the systems are Y2K remediated (do it yourself, or contact system administrator, system owner, or Year 2000 Council representative)
- Test systems and document results
- Report status to Group leader

3.3 Responsibilities of Other Specific Groups or Individuals

3.3.1 Facilities and Waste Operations (FWO) Division

- Manage A/E facility evaluation survey
- Assist with “zero hour” planning and execution
- Serve as advisor to Facility Managers for Year 2000 issues

3.3.2 ESH Division

- Assume primary responsibility for ES&H monitoring and reporting systems.

3.3.3 Johnson Controls of Northern New Mexico (JCNNM)

- Ensure Year 2000 compliance of IT and embedded systems for functions and equipment within area of responsibility
- Support the Laboratory in contingency planning and execution
- Support the Laboratory with remediation, testing, and verification where needed
- Participate in the facility evaluations by the contracted Architect/Engineering (A/E) Year firm
- Evaluate JCNNM facility system risk
- Prioritize JCNNM facilities and systems
- Do planning: determining resource needs, scheduling and executing Year 2000 renovation, testing, and implementation
- Allocate resources (money and people) for evaluation and repairs
- Develop contingency plans for your facility
- Prepare Year 2000 documentation according to the guidance (see Appendix A)

3.3.4 Protection Technologies of Los Alamos (PTLA)

- Ensure Year 2000 compliance of IT and embedded systems for functions and equipment within area of responsibility
- Support the Laboratory in contingency planning and execution
- Evaluate PTLA facility system risk
- Prioritize PTLA facilities and systems
- Do planning: determining resource needs, scheduling and executing Year 2000 renovation, testing, and implementation

4.0 Technical Aspects of the Year 2000 Problem

4.1 Year 2000 and IT computer systems

The magnitude of the problem may be hard to grasp: almost every computer system is subject to failure. In computer codes, two digits rather than four digits were frequently used to designate the calendar year (such as DD/MM/YY) to save valuable storage space and data entry time (just as people commonly refer to "the class of '96"). Although this has been common practice, it can lead to incorrect results whenever computer software performs arithmetic operations, comparisons, or data field sorting involving years later than 1999.

The Year 2000 date issue has the potential to affect not just the administration of operations, but also science and technology activities. There may be liability and ES&H issues at stake if systems fail. It is a big challenge for organizations as complex as LANL. Most systems need to be upgraded or patched. It's important to understand that even though a computer calculation may cause the problem, the effects can reach into other aspects (e.g., data collection, programmatic equipment, security, facilities). It is a layered problem; affecting hardware, operating systems, commercial applications, custom applications, and data interchange.

Most systems that will fail due to Year 2000 problems will all fail on 01/01/2000 or sooner. According to GartnerGroup, only 10% embedded systems will fail at or around the "zero hourSome systems may fail after Jan 1, 2000 due to leap year problems (the Year 2000 is a leap year), or monthly and quarterly processing requirements. Other systems will fail to collect data or execute a process because of a faulty date calculation.

Year 2000 failures could result in halting transaction processing, miscalculation of dates and date intervals, system functions halted or stopped, electronic data transfers inoperable, and unavailable infrastructure services such as power, telephones, and networks.

4.2 Year 2000 Embedded Systems in Programmatic Systems and Experimental Equipment

Many real-time systems used for programmatic or compliance activities also require upgrades or patches. Some of these systems are PC based and face the same issues as computer systems. A few of these systems were implemented in the 1980s and require a total replacement. The Laboratory cannot operate within the prescribed safety or security envelope unless these embedded systems are operational.

4.3 Year 2000 Embedded System in Facility Systems and Equipment

Embedded systems operate or control facility equipment. Examples include HVAC (heating, ventilation, and cooling) and SCADA (supervisory control and data acquisition systems). The Year 2000 errors will occur when the Laboratory is closed for the winter holiday break. This leaves our facility assets vulnerable during the coldest part of the year. We need to locate these systems, and develop solutions, workarounds, and facility contingency plans to mitigate our risk.

The Facility survey analyzed 160 buildings and found that almost 9 percent of the facility systems had Year 2000 issues. This information was entered into a spreadsheet and provided to the appropriate Facility Manager. The FM assigned the system Year 2000 criticality, then the spreadsheet data was uploaded into the Year 2000 database.

5.0 Year 2000 Requirements

5.1 Inventory Your Essential Systems

A comprehensive inventory of systems used by each line organization is critical for understanding the complete picture for Year 2000. In a line organization, the inventory contains all computer systems, applications, and programmatic equipment. In a facility, the inventory contains all facility systems.

5.2 Rank Systems According to Risk

Ranking inventoried systems by risk prioritizes the Year 2000 activities and provides increased focus on critical and important systems. Appendix D offers guidance for assessing the risk of the system. System owners, customers, and managers must come to agreement on the risk ranking of the systems.

5.3 Develop Plans for Noncompliant Systems

Plans should define the work to be performed, the resources (money and people), and milestones to measure progress against the plan.

5.4 Renovate Noncompliant Systems

Noncompliant systems are renovated using a six-step method: repair, replace, replace with commercial off-the-shelf software (COTS), establish a temporary work-around, remove, or no action. 'No action' may be appropriate if there are no time dependencies associated with the system and the failure would not be catastrophic.

5.5 Test

Testing Year 2000 is a complicated activity and must be planned carefully to mitigate side effects. There is not just one date to test for. The critical dates to test are listed in Appendix E.

5.6 Implement

Implementation occurs when the renovated system is put into place for regular use. This is the most important date in Year 2000 remediation and is our key milestone to measure progress.

5.7 Develop Contingency Plans for the Most Critical Systems

There are so many unknowns with Year 2000 that a contingency plan is required for the most critical systems. Many critical systems already have general contingency plans in place. The existing plans should be reviewed because some plans may need special provisions for Year 2000. The system owners should develop plans where they do not exist.

5.8 Document Progress and Compliance

Each system that has Year 2000 issues should have accompanying documentation that shows the findings, plans, renovation, test, and test results. There are no hard-and-fast rules for documentation; a best-practices approach should be followed. Guidelines for documentation are in Appendix A.

6.0 Year 2000 Schedule Requirements

The Year 2000 project schedule (Appendix G) follows the risk-based approach that will assure that the Laboratory is prepared for the Year 2000 by the end of FY99.

6.1 DOE Mission-Essential Systems

Note: A description of each of the four DOE mission-essential systems is in Appendix F.

All mission-essential systems must meet the DOE HQ Year 2000 program schedule. This schedule (Table 1) contains the following milestones:

Table 1.
DOE Mission-Essential Systems Year 2000 Milestones

Category	Milestone date
Remediation	September 15, 1998
Validation	February 15, 1999 (recently changed to January 31, 1999)
Implementation	March 31, 1999
Contingency planning	April 30, 1999 (required for systems that miss the validation or implementation schedule) August 30, 1999 (for systems that meet the March 31, 1999 implementation milestone)

The Laboratory is ahead of the DOE mission-essential schedule requirements (see Table 2). Two mission-essential systems, MASS and BRASS, are scheduled for implementation in December 1998. CARLA is scheduled for March 1, 1999, but we expect the system to be implemented early. Only the Secure ICN is scheduled for implementation on the DOE due date, March 31, 1999.

Table 2.
Estimated and Actual Year-2000 Readiness Milestones for Laboratory Mission-Essential Systems

Milestones	BRASS	CARLA (CLOCS)	MASS	SECURE ICN
Est. Renovation date	8/28/98	9/14/98	8/15/98	9/15/98
Actual Renovation date	8/26/98	09/10/98	2/27/98	9/15/98
Est. Validation Date:	10/31/98	1/31/99	11/15/98	2/15/99
Actual Validation date	10/21/98	11/04/98	4/1/98	2/12/99
Est. Implementation date	12/24/98	3/01/99	12/31/98	3/31/99
Actual Implementation date	12/23/98	6/30/99	3/31/99	3/31/99

6.2 All Other Systems

Following the risk-based approach, the criticality of the system determines the due date for Year 2000 implementation. The Year 2000 Council is trying to comply by ensuring that systems will be Y2K-ready according to the schedule in Table 3.

Table 3.
DOE Year-2000 Readiness Schedule for All Systems

System Category	Implementation due	Contingency plan due
Critical	June 1999	August 1999
Important	August 1999	October 1999 (where needed)
Noncritical	September 1999	N/A

7.0 Year 2000 Contingency Plans

The Year 2000 date rollover has never happened before, and the effects of this unique situation are unknown. Everyone must be diligent about testing and preparing contingency plans for critical systems.

The Energy Facilities Contractors Operations Group (EFCOG), a group of DOE contractors nation-wide, has a Year 2000 working group that is sharing information on contingency plans. EFCOG Year 2000 solutions will eliminate a lot of duplication of this effort by each site.

Table 4.
Year 2000 Contingency Plan Milestones

Plan	**Completion Date**
Contingency Plans (Line organizations and Facilities)	August 1999
Institutional Plan (Laboratory-wide)	August 1999

8.0 Year 2000 Tracking and Reporting

8.1 DOE requirements

The four LANL "DOE mission-essential Year 2000 systems" are tracked in the DOE Headquarters (HQ) Year 2000 database. The Laboratory Year 2000 Project office updates the database with schedule and status information each month. DOE HQ Year 2000 Project ranks mission-essential systems as being 'at-risk' if milestones are not met or if the current schedule deviated from the baseline schedule.

The Laboratory is required to also report on the other Laboratory systems and facilities. Every quarter we report the following information as shown in Table 5. The source of this information is the Year 2000 Council's database. As we move closer to 2000 and make progress, the Number Completed is expected to reach the Total Number.

Fill in this table with information from the database or refer to the database?

Table 5.
Year 2000 Tracking Sheet for Systems

System Category	Total Number	Number Assessed	Number Completed
Non-mission essential applications	278	278	278
Embedded systems	1619	1619	1619
Telephone systems	21	21	21
Networks	26	26	26
Host/Servers	202	202	202
Workstations	873	873	873
Building systems	224	224	224
Biomedical devices	0	0	0
Laboratory systems	137	137	137

The Laboratory is also required to report information about data exchanges in its quarterly report. A data exchange in this context is defined as an electronic file that contains dates, sent to or received by an agency or company outside the Laboratory, except for DOE. The report contains the information shown in Table 6: From July through September 1999 the Laboratory also sent weekly Year 2000 status reports to the DOE.

Table 6.
DOE Data Exchange Requested Information

Exchange Partner	Number of exchanges	Number of Exchange Partners Contacted	Number of Compliant Exchanges
State/Local	0	0	0
Private Organizations	28	28	28
Foreign/International	0	0	0
Federal Government (not DOE)	19	19	28

The DOE HQ Year 2000 Program Office consolidates and reports these data to the OMB every quarter. OMB assesses all government agencies in their Year 2000 efforts and ranks the agencies. In the November, 1999 OMB report, DOE achieved an "A" score.

8.2 Year 2000 Database

The Year 2000 Council members or their designees use the Year 2000 database to enter and track systems in their division. The Council members work with system owners and managers to determine the inventory and assessment. All Year 2000 Council members update the schedule and track the progress for their group or division.

A 'system' in the database can be an individual system (e.g., a major application, a host or server, a building system) or a logical clustering of machines, like PCs and workstations. Each cluster of systems also has a quantity associated to account for the number of devices in the cluster.

The Year 2000 database accepts entry any time, but all information for the division or program should be entered by the 3rd Friday of the month. Reports are cut and available to management no later than the 4th Friday of the month.

The Year 2000 status was reported to division leaders each month until June 1999. Beginning in June, 1999, division leaders received weekly status reports. Graphical information was posted to the Year 2000 home page each Friday.

8.3 Year 2000 Barometer

A barometer for Year 2000 is a quick-look progress indicator to management, the Year 2000 Council, and others. The barometer tracks the following metrics:

- Number of systems
- Number of systems assessed
- Number of systems completed

Appendix A: Year 2000 Documentation Guidelines

Documentation of what has been done to prepare systems for the Year 2000 are important for several reasons. One is that documentation would offer proof of honest effort to repair a system and thus would provide legal protection. It is also important that the written test plan be available to retrace repair steps should there be problems with a system.

The documentation should include, at a minimum:

- System name
- Description
- System owner
- Hardware description
- Operating system(s)
- Applications
- Data Exchanges
- Year 2000 Problems & Solutions
- Test plan
- Test plan results
- Contingency plan (if appropriate)
- Schedule (to serve as proof of plan and execution)

Appendix B: Year 2000 Computer System Evaluation Guidelines

System Layers and the Year 2000
Will your system work in the Year 2000? This question may seem easy until you consider the layers within your system that may be affected. You will not be home free until you have ensured that all of the five layers described below will handle the date changeover correctly. To follow up on the information given here, use the resources found at the IA Year 2000 Web site located at htttp://www.lanl.gov/projects/ia/year2000/.

Layer 1: Hardware

The bottom layer is the chip itself. Here are some status reports:

--All Mac chips are Year 2000 compatible.
--The Intel 286 chip will not boot when the Year 2000 comes. The chip gets so confused that it will not start the computer. Most Intel 386 and 486 chips used in PCs before 1995 will also have problems.
--Even some Intel PENTIUM chips have problems because of the way the chip is integrated into the PC motherboard. The Intel Web site (http://support.intel.com/support/year2000/) includes a reference list by motherboard serial number that indicates which PCs have chip problems and what upgrades or patches may be required.
--Hardware that is over 5 years old is highly suspicious.

Layer 2: Operating Systems

The next layer is the operating system (OS). The OS is the main control program that runs the computer. It runs continuously, sets the standard for running applications, and resides in memory at all times. The following information is a starting point:

All versions of Mac OS are Year 2000 compliant.
Every other operating system needs to be upgraded.
Manufacturers are issuing patches frequently, so continue to check for new patches and releases.

Level 3: Commercial Applications

The middle layer is commercial off-the-shelf software purchased from software companies. These applications may require you to purchase the latest release to be Year 2000 compatible. They include the following:

CAD software.
Geographical Information Systems (GIS) software
Graphic and Imaging software
E-mail packages.
Word processing systems.
Database systems.
Code development software (e.g., compilers).
Code management systems (e.g., PVCS).

Current Year 2000 status of these products are provided on the IA Year 2000 Web page. If your software is not listed, please send email to ia-year2000@lanl.gov. The IA Year 2000 staff will research the product, give you an answer, and post the product on the web site for use by others.

Layer 4: Custom Applications

Software developed at the Laboratory comprises the fourth layer. This layer is more complex and costly to fix because a software developer must find the source code and look for dates in the code. The programmer must also look at what computations and sorting are performed on those dates. Often the code must be modified to function correctly, but you must first answer the following questions:

Will the application accept "00" as a valid year?
What calculations are performed based on the date?

Custom applications should be thoroughly tested to assure compliance.

Layer 5: Data Exchange

The final layer is data exchange. Ask yourself the following questions about the files your application receives or sends:

Do the files have dates in them?
Will the date be expanded to a 4-digit year? If so, when?
If the date is not expanded, what agreement exists between the sender and receiver of the file?

Don't be surprised if you suddenly start receiving files with two extra characters in the date field to indicate the century. Even though this practice should not be unexpected, it would be better if the sender of the file communicated with the receiver beforehand about the specific practice being used.

Some systems use windowing to represent a date. Using this practice, any year designation less than "50" is preceded with "20" (e.g., 2049); dates greater than or equal to "50" are preceded with "19" (e.g., 1950). This is a valid practice and a good solution in many cases. But again, it is important that this agreement be made explicit and not assumed. A sample agreement letter is on the Year 2000 web site for your convenience.

Summary:

Hardware

PCs must be tested
5+ years old are highly suspicious
Check with the manufacturer using Year 2000 web site
BIOS/RTC test on PCs using Y2K from ESD

Unless you are running Mac OS you need an upgrade or patch

Check with the manufacturer using Year 2000 web site

Commercial software

Typically, only latest release is supported
Check with the manufacturer using Year 2000 web site

Custom software

Check for storage format for date, and how dates used
Sorting, calculation, scheduling algorithms
Look for dates used as keys (e.g. documents are keyed with date of receipt)
Testing is the only way to assure that the custom application will operate correctly in 2000.

End users should check with applications developer

Data exchanges

Evaluate all files with dates or dates used as part of the filename
Either write a letter or change file format or filename

End users should check with applications developer

Appendix C : Year 2000 Embedded System Guidelines

What is an embedded system?

An embedded system is a device that uses a processor or set of processors, but is not commonly thought of as a computer. Some embedded systems are PCs, and therefore have all the PC hardware and operating system Year 2000 issues. These systems are often used for data collection, experimentation control, or building system control, and are often hidden within the laboratory or facility. The Laboratory has embedded systems in facility systems and programmatic equipment. These systems should be evaluated for Year 2000 vulnerabilities.

Examples:

- SCADA (supervisory control and data acquisition)
- DCS (distributed control system)
- BMS (building management systems)
- Laboratory equipment
- Environmental monitoring systems

The microcontroller could be called a "one-chip solution." It typically includes:

- CPU (central processing unit)
- RAM (Random Access Memory)
- EPROM/PROM/ROM (Erasable Programmable Read Only Memory)
- I/O (input/output) - serial and parallel
- timers
- interrupt controller

What might happen in the Year 2000?

Most embedded systems are concerned with "NOW" and are used to monitor the time between events. The following examples of a one hour interval illustrate how the second interval may not be detected across the 2000 boundary.

- 00/01/01 01:15:00 to 00/01/01 02:15:00
- 99/12/31 11:15:00 to 00/01/01 00:15:00

Questions to ask about whether or to be concerned about an embedded system failing in the Year 2000:

1. Is it older than 1975?
Probably don't need to look further unless newer design equipment installed through maintenance.

2. Does it contain digital equipment?
If yes, then ask questions 4-7.

3. Does it interface with or is it calibrated with digital equipment?
If yes, then ask questions 4-7.

4. Does it or the interface equipment contain a processor &/or memory?
If yes, then, the item should be inventoried as a system (or specifically included in the scope of an already inventoried system).

5. Does it or the interface display a date?
If yes, then the item is vulnerable to the date problem, the item should be inventoried as a system (or specifically included in the scope of an already inventoried system)

6. Does it or the interface have a menu function to set date?
If yes, then the item is vulnerable to the date problem, the item should be inventoried as a system (or specifically included in the scope of an already inventoried system).

7. Does it or the interface have a clock battery for maintaining a reference time?
If yes, then the item is vulnerable to the date problem, the item should be inventoried as a system (or specifically included in the scope of an already inventoried system).

What are some other resources available to get information?

EDS
http://www.vendor2000.com/framhome.htm

Mitre
http://www.mitre.org/research/y2k/docs/Y2K_DOWNL

GSA
http://y2k.lmi.org/gsa/y2kproducts/search.htm

Washington State
http://www.ga.wa.gov/y2k/index.htm

IEE Year 2000
http://www.support2000.com/mpos.htm
http://www.iee.org.uk/2000risk/Welcome.html

Appendix D: Risk Assessment Guidelines

Risk Assessment Matrix

	Critical	**Important**	**Non-Critical**
The Mission	Unable to perform or Major disruption / delay	Minor disruption or delay	No disruption or delay
Health & Safety	Death or Major illness or injury	Minor illness or injury	No illness or injury
Security	Major Security Concern	Minor Security Concern	No Security concern
Environment	Irreversible or Major environmental damage	Minor environmental impact	No environmental impact

Appendix E: Year 2000 Testing: What are the Critical Dates?

Beginning of the year:

1/1/1999
1/1/2000
1/1/2001

End of year:

12/31/1998
12/31/1999
12/31/2000

Leap year:

2/28/2000
2/29/2000
3/1/2000

Date rollover (power off and power on):

Set date to 12/31/1999 at 11:55 PM; ensure that the date and time roll over correctly (power off and power on)

Possible bounds test or "never expire" tests:

9/9/99 (some applications use 99999 to mean "never expire")
9/10/99

Date crossing test:

12/31/1999 to 1/1/2000
2/28/2000 to 2/29/2000
2/29/2000 to 3/1/2000
12/31/2000 to 1/1/2001

Julian date:

2000060 or 00060 is Feb 29, 2000
2000366 or 00366 s Dec 31, 2000

What to look for:

1. Dates embedded as part of other fields
2. Dates used for sorting
3. Dates used as part of a file name
4. Dates used to trigger another process (e.g., deleting old e-mail)
5. Processes that are triggered by dates (e.g., routine maintenance forecasting, expiration dates, weekly and monthly processes).
6. Validate external system interfaces or file exchanges:
7. If date is expanded to 4-digit year be sure that a file exchange test is completed
8. If date is not expanded, agree with your other party on data window for century. Implement

Appendix F: Los Alamos National Laboratory DOE Mission-Essential Systems Descriptions

CARLA (CLOCS) The Classified Records System (CARLA) will be replaced with document technology and is called CLOCS (Classified LOCATES). LOCATES, an unclassified version of this system, is operational in CIC-10. CLOCS manages the centrally held classified document collection and uses Documentum, Lotus Notes, and Oracle.

Secure ICN The Secure ICN is the Los Alamos classified computing environment focuses on satisfying the needs of the weapons program. It includes the hardware and software for our networks, supercomputers, file systems, and output systems. This is a highly integrated and complex set of 33 components. The CIC High Performance Computing Focus Team has chartered its own Year 2000 working team to examine and coordinate the Year 2000 ICN migration, both Secure and Open. This team will coordinate the plans with the component owners, paying special attention to the interdependencies of the ICN components. The team's first priority is the Secure ICN. The Open ICN will follow.

MASS The Nuclear Material and Accountability System (MASS) tracks all nuclear material at the site. Without MASS, LANL cannot transport any nuclear material, both within the site and outside. MASS runs on a Tandem computer system and is maintained by the same staff at NMT that developed the system over the last 20 years.

BRASS The Secure Alarm System controls the alarms and access control devices to the secure areas. Most of the hand geometry badge readers are controlled by BRASS. BRASS is integral to the Laboratory's physical security program.

Appendix G

December 1999 Year 2000 Project Update

Year 2000 Project Update December, 1999

DOE safety-related systems

The data on safety-related systems require some explanation. To begin with, a safety-related system is one that is referenced in an "authorization basis" document. In January, DOE HQ gave the Laboratory a list of 9 "nuclear" facilities that required the safety-related system assessment. The Director's office deleted two facilities, LANSCE and DARHT, because they are not nuclear facilities, leaving 7 facilities for study. On April 7, 1999, DOE HQ issued revised guidance calling for identification of all safety-related systems at the Laboratory. The Laboratory had a false start in this process because of the initial definition of the 7 nuclear facilities that required study. However, during the June 3 DOE HQ site visit, DOE LAAO pointed out that we had 19 nuclear facilities. Subsequently, three high- to moderate-hazard facilities were also identified, bringing the total to 22 facilities for study. As a result of these developments, we negotiated a new due date (August 30) for all safety-related milestones. Once we understood the facilities of concern, we identified their systems that used dates for processing or data collection. Of the 160 systems examined, 18 had digital components with date sensitivity; of these, 7 systems required Year 2000 repairs and 11 did not. The DOE/AL independent verification and validation (IV&V) safety system assessment stated that "Los Alamos National Laboratory has adequately identified safety system that require Y2K attention." The August DOE HQ review applauded the Laboratory approach to defining safety-related systems and our use of independent experts in validating those systems.

All safety-related system negotiated milestones were met or a DOE/AL approved exception was in place by August 30. We used established risk criteria (see Appendix D) to determine which systems were critical and important and should therefore receive the most attention. The 18 safety related systems are listed below.

	DOE HQ SYSTEM ACRONYM	SYSTEM NAME
1	CMR-CAMS	CMR CAMS*
2	HCF-CAMS	Hot cell facility CAMS
3	LANS-EMS	LANSCE emissions monitoring system
4	RAMROD-CAMS	RAMROD CAMS
5	RANT-CAMS	RANT CAMS
6	RLW-CAMS	Rad liquid waste CAMS
7	RLW-MLD	RLW-manhole leak detection
8	RLW-VENT	RLW liquid waste ventilation
9	TA54-CAMS	TA-54 CAMS
10	TA54-DVS	TA-54 drum vent system
11	TA55-FCS	TA-55 facility control system
12	TSFF-UPS	TSFF-UPS
13	TSTA-MDAC	TSTA-master data acquisition and control
14	WCRR-CAMS	WCRR CAMS
15	WCRR-DDC	WCRR digital data controller
16	WETF-AD	WETF Auto Dialer
17	WETF-HVAC	WETF HVAC
18	WETC-IC	WETF instrumentation and control

*CAMS (continuous air monitoring system)

Other Activities

Laboratory Year 2000 Web Site
The Laboratory Year 2000 Web site (http://www.lanl.gov/projects/ia/year2000/) provides information on product readiness, testing, embedded systems, and FAQs for specific Laboratory systems as well as tips of the week on specific remediation issues and links to other useful sites. More than a dozen other Year 2000 sites are linked to our Web site, including the DOE CIO Year 2000 site. DOE has recognized our Web site as providing "an excellent source of information on PC/Windows, Macintosh, Unix, Networks, and Embedded System products." Our site was also recognized by the American Waterworks Association as one of the "Best Year 2000 Sites" http://www.awwa.org/y2k05.htm

Year 2000 Awards Program
The Year 2000 Project office sponsored an awards program to recognize individuals and teams who had done outstanding remediation work on Year 2000. More than $90,000 was awarded to Laboratory employees and contractors. The list of recipients and projects is located on the Year 20000 Web site: http://www.lanl.gov/projects/ia/year2000/docs/winners.html

CIC Year 2000 SWAT Team
CIC division formed a SWAT (special weapons and tactics) team to pinpoint resources with the Laboratory for desktop computing issues. The SWAT team project plan follows.

CIC Year 2000 SWAT Team

Project Plan

1.0 Purpose

The CIC Year 2000 SWAT team purpose is to develop and implement an overall unified strategy to provide computer customer support both prior to and following the rollover to Year 2000. The SWAT team will seek to minimize interruptions to operations of noncritical computers, and to ensure rapid recovery following the rollover.

2.0 Scope

The CIC SWAT team will be active for a limited time period and will be limited to addressing Y2K issues for primarily noncritical computer systems, largely desktops and NT servers. The time period covered is November 1999-January 2000, with emphasis on the first weeks in January especially when the Laboratory reopens on Monday, January 3, 2000.

3.0 Goals

The primary goal of the CIC Year 2000 SWAT Team is to limit the impact of Y2K on our customers and support services.

4.0 Approach

4.1 Base on Risk

The CIC SWAT team will use a risk-based, triage approach when deciding what order to handle customers. Triage is defined as "the sorting of and allocation of treatment to patients according to a system of priorities designed to maximize the number of survivors." In this case, it will mean prioritizing response based on impact and customers.

Call structure: The CIC-6 voice mail answering system will be reconfigured in preparation for rollover.

4.2 Educate

- Make available on Web a presentation to X Division How to Test Your PC for Year 2000" (RealMedia 45-min video clip)
- Improve, add to, and publicize Y2K Web site
- Publish useful information for customers on Year 2000 in Laboratory publications (BITS articles, News Bulletin, etc)
- Issue IA Advisories on Year 2000

4.3 Limit Non-Y2K Problems

- Thanksgiving Shutdown

  The CIC Year 2000 SWAT team will recommend that Laboratory nonessential computer systems be shut down (powered off) when users leave for the Thanksgiving weekend. The "power up" after Thanksgiving will reveal any problems that a shutdown might cause and would identify these issues apart from the rollover to Year 2000. Because users so seldom turn off their machines, many system features may have never been tested through a full cycle of power off and back on.

4.4 Limit use of CIC Call Center

- The CIC Call Center will take advantage of the LANL Y2K Website
- Current site improvements
- Determine when call center can point customers to it.
- Post rollover bug fix area addition
- Computing status page: combine and simplify existing ICN status pages
- Year 2000 product user guides
- In the event of cascading disruptions the SWAT team will create an E-mail distribution list for notification of Year 2000 news and recommendations.

4.5 Coordinate with the Year 2000 Council

The Year 2000 Council is made up of knowledgeable computer users from most divisions and program offices at the Laboratory. The Council has an E-mail distribution list for and by this means, information on Year 2000 issues can quickly reach a large population quickly.

5.0 CIC SWAT Team

5.1 Membership

The CIC SWAT team consists of at least one individual from each of the following organizations:

- CIC-2: Desktop
- CIC-6: Customer Service
- CIC-13: Business Information Systems
- CIC-15: Database and Information Technologies

5.2 Responsibilities

The sheer volume of computers at the Laboratory requires that we develop support teams that will help solve Year 2000 problems for customers in January 2000. The non-critical systems and individual workstations may not function properly. CIC should be prepared for an onslaught of calls from customers with Year 2000 problems. A SWAT Team from CIC-2 (desktop), CIC-6 (consultants), CIC-13 (Lab wide systems), and CIC-15 (Database Technologies) should be chartered in early 1999 to learn about the problems customers will have and devise strategies and solutions that help the customer solve their problem quickly. The better CIC is prepared, the faster the customer can be productive.

Industrial and Business Development Software Disclosure
The Year 2000 Project worked with the Civilian and Industrial Technologies Program Office(CIT-PO) (now IBD, industrial and business development) to develop a Year 2000 Readiness Disclosures survey and Web site for software that has been developed at the Laboratory and distributed externally. The Web site gives the status of the software's Year 2000 readiness. http://ext.lanl.gov/orgs/citpo/forms/y2kform.html

Year 2000 Communications and Outreach
Finally, we have used a variety of means, including articles, presentations, posters, and brochures, to communicate information on both personal preparedness and readiness issues within the Laboratory. Diane Weir, the Year 2000 Project leader, has given at a variety of Laboratory forums, to the All Managers Meetings, and to groups and divisions within the Laboratory. In addition, she has spoken to many community groups in northern New Mexico on Year 2000 preparedness. With Chuck Pacheco of the Laboratory Community Relations Office, she helped the City of Santa Fe with its Year 2000 Summit, held in December 1998.